Ascertaining Authenticity of Battery-Powered Devices in Avoidance of Interaction with Honeytrap Systems via Voltage Analysis and Special Imprinting

10 May 2025
Simon Edwards
Research Acceleration Initiative

Introduction

It is now a standard practice; particularly for nation-state entities; to employ what are known as “honeytrap” computer systems in a position which is logically separate from the true location of networked devices. The intent of these systems is to allow a prospective cyber-intruder to believe they are interacting with a genuine target network or device whereas they actually interacting with a system containing no data of value and interaction with which is heuristically analyzed in order to allow for information concerning the methods (code) used to support the intrusion to be collected in order to both identify and prevent future attacks. This also buys time to track down the origin of an intrusion and to conduct a counter-intrusion in real-time, in some cases. This technique can be used to protect an entire network or an individual device. Occasionally, the devices being protected by these methods are battery-powered i.e. they are either laptops or cellular telephones.

In many cases, if an individual is identified as a ripe target for surveillance in a foreign country, for example, a nation-state actor may wish to collect information concerning the communications and travel of a particular person of interest. Oftentimes, if the personal electronic device of said person is infiltrated, it may take weeks, months, or even years before the infiltration is noticed. When it is noticed, however, the nation-state to which the targeted individual belongs may attempt to mislead a hostile entity by beginning to present the hostile entity with a virtualized copy of the targeted individual’s device which is, in actuality, a honeytrap which is implemented *ex post facto.*

As ex post facto honeytraps present an increasingly relevant challenge for those concerned with offense cyber-operations, novel methodologies are required which allow both for authentic systems to be differentiated from honeytrap systems as well as which allow for specifically targeted systems to be “marked” for later re-acquisition. This paper addresses itself to one such possible technique.

Abstract

The ability to control and monitor the voltage flowing into or out of a battery is an incredibly valuable asset for a cyber-intruder. Historically, this access has been used to in order to, for example, purposefully over-charge batteries in order to cause explosions and has, as this author has pointed out, been used in order to transmit data covertly without the need to send packets (in the case of the voltage control systems in routers rather than in voltage cells.)

When a battery-powered device is used, a voltage meter monitors the voltage in order to estimate how much energy remains. These observations are

usually simplistic and are taken at intervals of every few seconds. However, with slightly more affluent observations, information of much greater utility can be collected from the battery, the most obvious of which is that a given device is, in fact, being powered by an *actual* battery. In a virtualized "honeytrap" system, characteristic fluctuations associated with battery-powered systems are likely not to register with the voltage meter because there is no voltage meter and there is no battery.

Assuming that a honeytrap system emulates a native voltage meter, this emulation usually consists of only a steadily descending "% of full charge value" and does not emulate the subtle fluctuations associated with varying conditions of temperature, for example, seen in the real world. For example, in the winter, if an individual's phone is taken from indoors out to a vehicle when the temperature is cold, the temperature of the battery will drop, causing the apparent available voltage to suddenly decline until the temperature increases. Most phones have temperature sensors, but these are rarely emulated correctly.

More important than these more obvious potential weaknesses (for which certain entities may soon make improvements) of emulated systems are even less obvious characteristics of the voltage provided by batteries to electronic devices which are almost certainly not being reproduced by any honeytrap system. If the certain characteristics of charge are tampered with by an intruder, it could be expected that the discharge characteristics of the battery could be modified over the short-term (sc. within the context of a given charge cycle) so as to enable the intruder to use the voltage meter in order to confirm that a system is not only authentic, but to ascertain with which one of dozens or hundreds of "marked" systems they are communicating. For example, an intruder may increase charge voltage or may alternate charge voltages (ibid. this author's paper concerning extending the life of batteries using a similar method) in order to cause the battery to produce a measurable harmonic of voltages upon discharge.

Although the voltage meters shipped with cellular devices are not generally used to measure voltage harmonics in any great detail, with some slight software modifications, they could be made to do so. For example, a battery might produce voltage which averages 3.8 Volts, but which has either a wide or narrow range of tributary voltages which produce this average number. These harmonics can be represented in much the same way that the histograph of a digital image or of an audio recording may be, showing the volume of sound at each individual frequency. If the harmonics of the charge applied to be battery can be controlled by an intruder, the discharge harmonics could be made to correspond to the charge harmonics in a way which makes the battery uniquely identifiable within the context of an individual charge cycle.

What's more, even without this imprinting, an intruder would be able to ascertain readily whether the system with which they were communicating was being powered by an battery or was merely "pretending to be" battery-powered. If a system already under surveillance were to suddenly stop producing voltage with appropriate harmonic characteristics, this could be taken as a sure sign that an intrusion had been retroactively detected and that

a honeytrap system had been placed between the real device and the intruder in the hopes that the intruder would continue interacting as before and that they do not take steps to sever the connection. Monitoring voltage harmonics offers a given entity interested in maintaining offensive cyber-operations against battery-powered devices a quick and easy method for determining when to sever a connection in order to prevent counter-intrusion and fingerprinting.

Conclusion

An entity employing such techniques would be able to avoid interaction with intelligence-gathering honeytrap systems and would likely be able to track down the true logical location of target devices, provided that the nation-state entity even allows the person to continue to use the device after a compromise has been detected. This is the case more often than one might expect as it is necessary for the protected individual to be unwitting to a counterintelligence investigation in order to rule out the involvement of the targeted individual.

This method affords a given entity a clandestine capability both to detect deceptive computer networks and to mark devices of interest for later re-acquisition and its utilization is unlikely to be anticipated.